UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/804,258	03/13/2001	Hung-Che Chiu	MR2349-600	9125

4586 7590 09/24/2004

ROSENBERG, KLEIN & LEE
3458 ELLICOTT CENTER DRIVE-SUITE 101
ELLICOTT CITY, MD 21043

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/804,258	CHIU, HUNG-CHE	
	Examiner	Art Unit	
	Thomas M Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *13 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 are pending.

Claim Objections

2. Claim 4 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 3. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-2, 5-7 are rejected under 35 U.S.C. 112 second paragraph as being indefinite.

Regarding claim 1-2, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

For purposes of examination however, the first part of claim 1 shall be read as "An end to end real-time encrypting module of a mobile commerce WAP data transmission section, wherein the uppermost layer of the wireless application environment (WAE) is used as a developing platform and executing environment and is suitable for various communication

networks, *comprising at least one of GSM, PDC, CDPD, CDMA, TDMA, PHS, DECT, or GPRS* and third generation mobile phone (3G);"

For purposes of examination claim 2 shall be examined as if it read

The end to end real time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when a user registers into the WML server of WCP through a WAP network, the WML server will inform the cipher server to be responsible for actuating a public key remained in the handset software encryption and decryption module and the key management through the cipher server for the inter-process communication interface provided by operation systems of various computers; the public key is downloaded to the client, *comprising at least one of a mobile phone and a personal digital assistant*, using HTTP service through a WAP gateway of a WAN (wide area network), GSM/GPRS/CDMA and other digital mobile systems.

In reference to claims 5-7:

The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

For purposes of examination, the narrative explanations offered at the end of the claims will be ignored.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 7 as best understood, are rejected under 35 U.S.C. 102(e) as being anticipated by Puhl et al.

In reference to claim 1:

Puhl et al. (Figure 1) discloses

- an end to end real-time encrypting module of a mobile commerce WAP data transmission section, wherein the uppermost layer of the wireless application environment (WAE) is used as a developing platform and executing environment and is suitable for various communication networks, comprising at least one of GSM, PDC, CDPD, CDMA, TDMA, PHS, DECT, or GPRS and third generation mobile phone (3G), where these protocols are understood known to be runnable over the wireless application environment, since the wireless infrastructure and use of WAP data transmission is disclosed. (Figure 4, Items 450, 420)

- an information encryption code security system matching the public key infrastructure is installed in a WML server end of a current mobile server of a wireless service provider, where the WML server is the WAP proxy server which serves as a WML server in that it translates HTML into WML. (Column 3, lines 35-40)

- and the system includes a handset software encryption and decryption module, a cipher server, and a key management, where the software encryption and decryption module and cipher key is supported in the WAP PKI (Column 9, lines 22-30) & (Column 9, lines 29-50)

In reference to claim 2:

Puhl et al. discloses

- the end to end real time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when a user registers into the WML server of WCP through a WAP network (Column 10, line 65 – Column 11, line 5), the WML server will inform the cipher server to be responsible for actuating a public key remained in the handset software encryption and decryption module and the key management through the cipher server for the inter-process communication interface provided by operation systems of various computers; (Column 9, lines 38-50)

- the public key is downloaded to the client(Column 4, lines 64-55), comprising at least one of a as a mobile phone(Figure 1, Item 11) or a personal digital assistant, using HTTP

service(Column 3, lines 35-40) through a WAP gateway(Figure 1, Item 18) of a WAN (wide area network), GSM/GPRS/CDMA and other digital mobile system, where GSM/GPRS/CDMA are protocols that are understood to be able to run on top of the Wireless infrastructure provided with the mobile phones.

In reference to claim 3:

Puhl et al. (Column 9, lines 38-50) & (Column 10, line 7-22)

discloses the end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein when it is desired to downlink a personal commercial information, a user inputs a private key to be left in the stack memory of the mobile WAE environment as a standby key, when the WML server transfers the personal commercial information to be downlinked to the cipher server and information the cipher server to open the public key remained in the handset software encryption and decryption module and key management for executing an encryption algorithm in the server end in advance; then, the handset software encryption and decryption module and the encrypted data are downlinked to a client through the HTTP service; then, the private key remained in the WAE executing environment is used to decrypt the encryption data and then the decryption plain text is transferred to display the original form through a WML format document for performing the following processes, where Puhl et al. discloses this through the use of WML format documents (Column 3, lines 35-40) placed in the context of a secure electronic system(Column 9, lines 18-21), through the use of a WAP Public Key Infrastructure, where it is understood by those in the art that a Public Key Infrastructure consists of encrypting with a public key and decrypting with

the private key such as in the RSA algorithm(Column 16, line 60 – Column 17, line 5) – a reference disclosing more details of the RSA algorithm is given for the Applicant's convenience. (Schneier pgs 464-468)

Claim 4 is rejected for the same reasons as claim 3.

In reference to claim 7:

Puhl et al. (Figure 1). disclose the end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1, wherein in the security mechanism, the handset software encryption and decryption module is based on the WAE application layer, and thus it is used to interpret wireless markup language (Column 3, lines 35-40), and wireless markup script language. (Column 9, lines 30-40)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Puhl et al. and Schneier "Applied Cryptography"

9. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Puhl et al.

In reference to claim 5:

Puhl et al. (Column 9,lines 38-50) disclose the end to end real-time encrypting module of a mobile commerce WAP data transmission section as claimed in claim 1,

Puhl et al. however, fails to explicitly disclose responsibilities of the key management including:

a) key generation and conditions

b) sharing of the keys

Schneier "Applied Cryptography" (pgs 170-175) discloses the usage of several key generation techniques, including the usage of random-bit strings so as to make guessing of the key difficult. Schneier additionally states "Good keys are random-bit strings generated by some automatic process"

Schneier "Applied Cryptography" (pgs 181-182) also discloses sharing of the keys, which provides the advantage of recovering data even when the key is lost.

It would have been obvious to one of ordinary skill in the art to use the key generation and backup techniques of Schneier "Applied Cryptography" in order to generate keys that are difficult to guess and prevent the loss of encrypted data if the key(s) are accidentally lost.

In reference to claim 6:

Puhl et al. discloses all of claim 6 except wherein a precompressor serves to compress transmission data where the procedure of the compressor

a) dividing original data into several unit character string, and each character string has 8 or 9 characters

b) converting each unit character string into a decimal value;

c) converting each decimal value into a unit character string of hexadecimal system

d) dividing each unit character string of a hexadecimal system into two unit character sets

e) converting each unit character set into a decimal character code between 0~255

f) converting each character code directly into a respective ANSI character set.

In the aforesaid step a) to use 8 or 9 characters as a unit is based on the fact that the maximum data length supported by a mobile phone WAE executing environment is 64 bits, if the data is represented by a decimal system, it has a length of 10; therefore in order to avoid data from overflowing, 8 or 9 characters is used as a unit.

The Examiner takes official notice that performing all of the above was well known in the art at the time of invention. Computers typically use the ASCII computer system in which represents characters as numbers which is converted through an ASCII table. Rarely if ever, are characters in a computer stored in decimal format. Instead values are stored as binary which, when grouped

into fours are rewritten as the well known Hexadecimal notation of base 16. ASCII numbers are also known to use 8 digit strings since 8 digits of binary can represent 2^8 – 1 values, or 255— the number of ascii values.

For Example, the character 'A' is known to be ascii value 65 as decimal. As Hexadecimal, this number is 41, which is represented in binary as 10000001, an eight digit character string.

It would have been obvious to one of ordinary skill in the art at the time of invention for the precompressor to represent the numbers using ASCII since that has been the standard of digital storage and character information that has permeated the computer science industry for the past twenty or thirty years.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TMH

September 17th, 2003